E-CMIRC: Towards a Model for the Integration of Services Between SOCs and CSIRTs

Pierre Jacobs1, 2, Sebastiaan von Solms2 and Marthie Grobler1, 2
1Council for Scientific and Industrial Research, South Africa
2University of Johannesburg, South Africa
pjacobs@csir.co.za
basievs@uj.ac.za
mgrobler1@csir.co.za

Abstract

Security Operation Centres (SOCs) and Computer Security Incident Response Teams (CSIRTs) or Computer Emergency Response Teams (CERTs) can play a pivotal role in the monitoring of, and response to threats, attacks and vulnerabilities in organisations, including governments. While the focus of a SOC is on the monitoring of technical security controls and critical assets, and the response to attacks and threats, CSIRTs' main focus is on response and incident management. One postulation is that a CSIRT or CERT is a highly specialised sub-capability of a SOC, whereas another postulation could be that a SOC serves as an input mechanism into CSIRTs and CERTs. In this paper, the differences between SOCs, CERTs and CSIRTs are established, and synergies between them are defined. This leads to an integrated services model for the establishment of an initial SOC and CSIRT capability in developing countries. Developing countries have unique challenges facing them where it concerns cybersecurity. Aspects such as Information Communication and Technology (ICT) infrastructure are often a challenge, and so is funding for ICT as well as skills. Political instability could also have an influence on the cybersecurity posture of developing countries by leaving developing nations open to malicious state-sponsored attacks. This SOC and CSIRT capability is made viable and possible through the savings in cost and resources by identifying overlapping services, as well as the application of the proposed model. This emergent SOC and CSIRT combined capability is called the Embryonic Cyberdefense Monitoring and Incident Response Center (E-CMIRC). The purpose of this paper is to identify a high-level integrated services model for the E-CMIRC in order to reduce cost and resources which serves as a barrier to entry in developing countries. A scalable operational framework is identified, and for the management of the effectiveness and efficiency, and also to ensure that all aspects of service delivery are considered, the Information Technology Information Library (ITIL) is proposed.